Remarks

Status of application

Claims 1-35 are pending in the subject application. The claims stand rejected on the basis of prior art. By this Amendment, Applicant has amended the claims in an effort to better distinguish the present invention. Re-examination and reconsideration of the amended claims are respectfully requested.

The invention

An electronic mail ("e-mail") system is described that provides methodology to enforce authentication or encryption to/from Mail Transfer Agents and from Mail User Agents. In accordance with the present invention, support is added to enforce certain restrictions on the connections between two hosts (a server and a client), depending on whether sendmail (Message Transfer Agent) acts as a server (receiving e-mail) or as a client (sending e-mail). In this manner, it is possible for each type of connection to enforce an authentication of the other side or at least a certain key length of the symmetric cipher used for encryption. Note in particular that these are additional restrictions, beyond any features provided by prior art SSL technique.

A method of the present invention for sending an e-mail message using a secured connection that employs encryption includes the following method steps. A client's request (e.g., Mail User Agent's request) is received at a Message Transfer Agent (MTA) for establishing a secured connection with the MTA for sending an e-mail message. The method attempts to authenticate the client, through use of a certificate. If the client cannot be authenticated, the method terminates without establishing the secured connection and without sending the e-mail message. On the other hand, if the client can be authenticated, the method establishes the secured connection between the client and the MTA. Additionally, the method (optionally) determines whether the encryption employed for the secured connection meets a predefined minimum encryption strength. If the encryption employed does not meet the predefined minimum encryption strength, the method terminates (including terminating the secured connection without sending the e-mail message). However, if the encryption employed does meet the predefined minimum

encryption strength, the MTA will send the e-mail message (for ultimate delivery at a target destination).

The above method can be modified so that the MTA acts as the client. In that case, the method is repeated with the MTA attempting to establish a secured connection with another server (e.g., second MTA). If the server can be authenticated, the e-mail message is transmitted on the secured connection. Otherwise, the secured connection is terminated. The first MTA (client, here) can (optionally) terminate the connection if the encryption strength is inadequate.

General

The Examiner has objected to the Abstract of the specification, for exceeding the current word count limit of 150. The Abstract has been amended to comply with the limit.

Prior art rejections

A. Section 102 rejection: Davis et al.

Claims 1, 2, 8, 12, 13, 16, 17, 23, 27, 28, 31, 34 and 35 stand rejected under 35 U.S.C. 102(e) as being anticipated by Davis et al. U.S. Patent No. 6,367,009 (hereinafter, "Davis"). The Examiner's rejection of claims 1, 16, and 31 is representative:

> As to claims 1, 16 and 31, Davis et al discloses receiving at a message transfer agent (MTA) a request from a client for establishing a secured connection with the MTA for sending an e-mail message [column 1, lines 52-55]. Davis et al discloses attempting to authenticate the client, through use of a certificate [column 11, lines 29-64]. Davis et al discloses that if the client cannot be authenticated, terminating the method without establishing the secured connection and without sending the e-mail message. Davis et al discloses that if the client can be authenticated, establishing the secured connection between the client and the MTA [column 12, lines 14-39]. Davis et al discloses determining whether the encryption employed for the secured connection meets a predefined minimum encryption strength. Davis et al discloses that if the encryption employed does not meet the predefined minimum encryption strength, terminating the secured connection without sending the e-mail message, whereupon the method terminates. Davis et al discloses that if the encryption employed does meet the predefined minimum encryption strength, sending the e-mail message [column 17, lines 9-34].

(Examiner's Action, paragraph 2.)

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in the single prior art reference. (See, e.g., MPEP Section 2131.) As will be shown below, the reference fails to teach each and every element set forth in claim 1, as well as other claims, and therefore fails to establish anticipation of the claimed invention under Section 102.

As pointed out by Davis, SSL (Secure Sockets Layer) is designed to provide several different but complementary types of security. For example, if a (human) user is buying goods over the Internet using a credit card, it is important for him or her to know that the application waiting on the other end of the connection for his credit card information is really the vendor he believes he is doing business with, and not an impostor waiting to steal his credit card information. As pointed out by Davis (as well as by others), SSL itself is certainly very well-known in the art and has a variety of applications.

Applicant does not claim to have invented SSL, whether used between a client and a server in an Internet e-commerce environment or use between a client and a server in an e-mail environment. In particular, Applicant's claims do not merely recite the use of SSL in conjunction with e-mail processing. Instead, Applicant's claimed approach uses SSL (or similar) but then enforces extra restrictions. Thus, the focus of Applicant's claimed invention is not the use of SSL per se but is the enforcement of the extra restrictions on top of SSL.

To be sure, SSL is an existing underlying technology that is used in Applicant's approach as well as in Davis' approach. However, in Applicant's system, the MTA attempts to enforce that the other side (e.g., client, or another MTA) does in fact have certain qualities, such as a certain certificate identity (i.e., is authenticated with a particular identity) and certain encryption strength. For example, during an attempted connection, the MTA may look up the certificate presented by the other side (client or another MTA) *for determining up front whether it even wants the connection.* In one embodiment, for example, the MTA looks up the certificate in its own table (of

acceptable clients or MTAs) in order to determine if it wants to grant the connection or not, based on the attributes of the presented certificate.

It will be appreciated that this is not simply establishing a SSL session between two entities, such as between an MTA and a client, or between two MTAs. Instead, during the exchange of certificates of an SSL session, the MTA consults its own list of acceptable entities for scrutinizing whether the presented certificate belongs to a party/entity (e.g., client or another MTA) that is a priori approved for connections. If the party attempting the connection is from an approved IP address, then the MTA allows the connection from anyone having a matching certificate name. Additionally, as part of this quality check, the MTA enforces a minimum encryption strength. For example, if the parties/entity attempting connection employs 40-bit encryption while the MTA requires 160-bit encryption, the attempted connection is rejected (on the basis of insufficient encryption strength). Importantly, the MTA may use an SSL-based approach to reject the connection itself based on the quality of the party attempting the connection. All told, SSL (or similar) is used as an underlying technology but then, in accordance with the present invention, the MTA enforces additional restrictions based on the quality of the presented certificates. The enforcement of these extra restrictions provide an improved authentication/encryption technique for connecting to/from a message transfer agent (MTA) that is not taught our suggested by the prior art.

The claims have been amended in an effort to bring these features to the forefront. For example, amended claim 1 now recites:

> receiving at a message transfer agent (MTA) a request from a client for establishing a secured connection with the MTA for sending an e-mail message;
> **attempting to authenticate the client, through use of a certificate, in order to identify the client as approved for establishing a secured connection with the MTA;**
> **if** the client **cannot be authenticated, terminating** the method without establishing the secured connection and without sending the e-mail message;
> if the client can be authenticated, establishing the secured connection between the client and the MTA;
> **determining whether** the encryption employed for the secured connection meets **a predefined minimum encryption strength;**
> **if** the encryption employed **does not meet** the predefined minimum encryption

strength, **terminating** the secured connection without sending the e-mail message, whereupon the method terminates; and
if the encryption employed does meet the predefined minimum encryption strength, sending the e-mail message.

(The other independent claims have been amended in a like manner.) As shown, the claimed method requires the use of the certificate to not only authenticate the client, but also in order to identify that the client is approved for connecting to the MTA. The section cited by the Examiner from Davis (column 12, lines 14-39) describes the mechanism where Davis' client establishes an SSL session with Davis' MTS. It does not describe that the MTS uses the client's authenticated identity (from the SSL certificate) for determining that the client is one that is already approved for establishing a connection in the first place. In conjunction with this determination, the claim requires that the connecting client meet a predefined minimum encryption strength. If these extra restrictions or conditions are not met, the MTA refuses the connection.

Turning now to the particular teachings of Davis, a careful review of the patent reveals that it does not describe the enforcement of extra restrictions on top of SSL, in the matter required by Applicant's claims. The Davis patent describes "extending SSL to a multi-tier environment using delegation of authentication and authority." Davis points out, "However, SSL was designed as a two-party protocol, to be used in a client/server environment. The SSL protocol provides for a client to request a secure communication session by sending a message to a server application." (Davis col. 2, lines 43-47.) As Davis focuses on "a technique whereby SSL can be extended into the three-tier architecture in a manner that allows the true client's identity to be known to the ETS," the Davis patented covers the extension of this two party protocol to three parties (see, e.g., Davis' FIG.6 - 8 and accompanying description).

With respect to Applicant's claimed invention, Davis provides little or no teaching beyond the base SSL art. Applicant's claimed invention uses SSL as a two-party protocol *only*. If there are three parties somewhere involved, then SSL is still only used directly between any two entities; there is no direct extension to three. Whether an MTA talks to another MTA or "users as client", the communication occurs between two parties. For

example in Applicant's specification, Fig.1 shows three parties but any particular connection occurs only between two parties at a given time. To get an e-mail from a client via one MTA1 to another, a two-party ("store and forward") approach is employed. The client firsts sends the message to its MTA1 and then that connection is terminated; the message is stored on the MTA1. Subsequently, the local MTA1 makes a new, unrelated connection to another MTA2. The client is never connected to MTA2, neither directly nor indirectly. The focus of Applicant's claims is the specific interaction between pairs of participants.

As described above, Davis provides little or no teaching that is relevant to Applicant's claimed approach involving two-party SSL communication, beyond commonly-known SSL technology of certificate exchange and encryption. Davis describes a scenario where the client makes a connection to a MTS (middle-tier server), the client then makes a connection to an ETS (end-tier server) while keeping both connections open, and then the client transparently talks to the ETS. This three-tier approach of Davis is completely different from the two party scenario in which any particular connection occurs only between two parties at a given time. E-mail is passed among successive pairs in a "store and forward" manner. More particularly, Davis provides no teaching relevant to the enforcement of the additional restrictions in a two-party SSL communication environment that are set forth in Applicant's claims. Accordingly, it is respectfully submitted that the amended claims distinguish over Davis and overcome any rejection under Section 102.

B. Section 103 rejection: Davis et al, Stille et al.

Claims 3, 4, 18 and 19 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al. U.S. Patent No. 6,367,009 as applied to claim 1 above, and further in view of Stille et al. U.S. Patent No. 5,878,397 (hereinafter, "Stille"). Stille is added by the Examiner for the proposition of teaching that a temporary error reply code may be returned.

The amended claims are believed to be allowable for at least the reasons stated above pertaining to Davis et al. Simply put, Davis does not describe Applicant's

enforcement of additional restrictions on top of two-party SSL-type communication, such as using the client's certificate identity in order to determine whether the client is already approved for the connection. Stille does not remedy this deficiency of Davis, and therefore it is respectfully submitted that the combination of the two references does not teach or suggest all of Applicant's claim limitations. Additionally, Stille describes his error code usage in the context of SMS (short messaging system) transmission, which differ significantly from e-mail. Stille does not describe usage in the context of e-mail systems. Accordingly, it is believed that the amended claims distinguish over the references and overcome any rejection under Section 103.

C. Section 103 rejection: Davis et al, Mulligan et al.

Claims 5 and 20 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et at U.S. Patent No. 6,367,009 as applied to claim 1 above, and further in view of Mulligan et at U.S. Patent No. 5,937,161 (hereinafter, "Mulligan"). Mulligan is added by the Examiner for the proposition of teaching that an e-mail message may be returned to its sender.

The amended claims are believed to be allowable for at least the reasons stated above pertaining to Davis et al. Simply put, Davis does not describe Applicant's enforcement of additional restrictions on top of two-party SSL-type communication, such as using the client's certificate identity in order to determine whether the client is already approved for the connection. Mulligan does not remedy this deficiency of Davis. Additionally, Mulligan describes his approach in the context of forwarding electronic mail messages. A given e-mail message is returned to the sender's address if a default delivery address is not entered into the system. The reference contains no description that the return of the message occurs in the context of the original sender failing to achieve an approved connection with an MTA (e.g., in a manner required by Applicant's claims). Quite simply, Mulligan does not describe return or "bounce" of an e-mail message at the point when the sender (client) is attempting connection to an MTA. Accordingly, it is believed that the amended claims distinguish over the references and overcome any rejection under Section 103.

D. Section 103 rejection: Davis et al, Landfield et al.

Claims 6 and 21 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et at U.S. Patent No. 6,367,009 B1 as applied to claim 1 above, and further in view of Landfield et at U.S. Patent No. 5,928,333 (hereinafter, "Landfield"). Landfield is added by the Examiner for the proposition of teaching that an e-mail mail message may queued for future sending if the client cannot be authenticated.

The amended claims are believed to be allowable for at least the reasons previously stated pertaining to Davis et al. above. Landfield does not remedy this deficiency of Davis. Additionally, Landfield describes (at the cited section) that e-mail messages may be stored within a message queue. Applicant's own Background section also indicates that prior art MTA's queue messages. The specific limitations set forth in Applicant's claims pertains to queuing of the message when the client cannot be authenticated. (The claim limitation does not relate to the general notion that messages may be queued.) The Landfield reference contains no description that the e-mail messages of clients that cannot be authenticated are queued up for future sending, as required by Applicant's claims. Accordingly, it is believed that the amended claims distinguish over the references, overcoming any rejection under Section 103.

E. Section 103 rejection: Davis et al, Gotta et al. .

Claims 7 and 22 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et at U.S. Patent No. 6,367,009 as applied to claim 1 above, and further in view of Gotta et at U.S. Patent No. 6,587,874 (hereinafter, "Gotta"). Gotta is added by the Examiner for the proposition of teaching that determining whether the encryption employed for the secured connection meets a predefined minimum encryption strength employing SASL (Simple Authentication and Security Layer) protocol.

The amended claims are believed to be allowable for at least the reasons stated above pertaining to Davis et al. As previously noted, Davis does not describe Applicant's enforcement of additional restrictions on top of two-party SSL-type communication, such as using the client's certificate identity in order to determine whether the client is already

approved for the connection. Gotta does not remedy this deficiency of Davis, and therefore it is respectfully submitted that the combination of the two references does not teach or suggest all of Applicant's claim limitations. Accordingly, it is believed that the amended claims distinguish over the references, overcoming any rejection under Section 103.

F. Section 103 rejection: Davis et al., Higley

Claims 9, 24 and 32 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al. U.S. Patent No. 6,367,009 as applied to claim 1 above, and further in view of Higley U.S. Patent No. 5,790,793 (hereinafter, "Higley"). Higley is added by the Examiner for the proposition of teaching a Mail User Agent (e.g., Microsoft Outlook).

The amended claims are believed to be allowable for at least the reasons stated above pertaining to Davis et al., for the reason that Davis does not describe Applicant's enforcement of additional restrictions on top of two-party SSL-type communication. Higley does not remedy this deficiency of Davis, and therefore it is respectfully submitted that the combination of the two references does not teach or suggest all of Applicant's claim limitations.

Additionally, it should be pointed out that Mail User Agents (MUAs) such as Microsoft Outlook or Eudora are of course well-known (and described in Applicant's Background section). However, the claim limitations are not drawn to simply claiming MUAs. Instead, the claim limitations require that the client that is participating in this process where extra restrictions are applied (e.g., on top of SSL) is a MUA. Higley does not describe this particular interaction between an MTA and an MUA, and thus does not include any competent teaching in regards to Applicant's claim limitation in these dependent claims. Accordingly, it is believed that the amended claims distinguish over the references and overcome any rejection under Section 103.

G. Section 103 rejection: Davis et al., Higley, Dickinson, III et al.

Claims 10, 11, 25, 26, 29 and 33 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et at U.S. Patent No. 6,367,009 B1 as applied to claim 1 above,

and further in view of Dickinson, III et al. U.S. Patent No. 6,609,196 (hereinafter, "Dickinson"). Dickinson is added by the Examiner for the proposition of teaching an e-mail system that uses SMTP, and that the MTA may comprise a Sendmail-compatible Message Transfer Agent (MTA) controlled, at least in part, by a configuration file for the Sendmail-compatible MTA

The amended claims are believed to be allowable for at least the reasons stated above pertaining to Davis et al. and Higley. Dickinson does not remedy this deficiency of Davis and Higley, and therefore it is respectfully submitted that the combination of all of the references does not teach or suggest all of Applicant's claim limitations.

H. Section 103 rejection: Davis et al., Heiner

Claims 14, 15 and 30 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al. U.S. Patent No. 6,367,009 B1 as applied to claim 1 above, and further in view of Heiner U.S. Patent No. 6,112,227 (hereinafter, "Heiner"). Heiner is added by the Examiner for the proposition of teaching a system that may reject at least some subsequent SMTP commands received from the client.

The amended claims are believed to be allowable for at least the reasons stated above pertaining to Davis et al., as previously stated. Heiner does not remedy this deficiency of Davis, and therefore it is respectfully submitted that the combination of the two references does not teach or suggest all of Applicant's claim limitations. Additionally, Heiner (which describes a junk e-mail filter) clearly describes that the deletion of unwanted e-mail occurs after it has already been received at the destination SMTP server: "If the source client's e-mail address is on the reject list, the e-mail message is deleted by the destination SMTP server, as indicated in step 110." (Heiner column 3, lines 31-35.) At the point that the destination SMTP server has already received the junk mail, it has already completed its SMTP communication (with the prior machine). One can hardly assert that that approach is the same as rejecting the SMTP communication up front (i.e., refusing the communication up front and certainly not accepting any such e-mail at the destination), as required by Applicant's claim limitations. If anything, Heiner teaches away from Applicant's claimed approach. Accordingly, it is believed that the

amended claims distinguish over the references and overcome any rejection under Section 103.

Conclusion

In view of the foregoing remarks and the amendment to the claims, it is believed that all claims are now in condition for allowance. Hence, it is respectfully requested that the application be passed to issue at an early date.

If for any reason the Examiner feels that a telephone conference would in any way expedite prosecution of the subject application, the Examiner is invited to telephone the undersigned at 408 884 1507.

Respectfully submitted,

Date: May 14, 2004

Digitally signed by John A. Smart
Date: 2004.05.14 15:00:41 -07'00'

John A. Smart; Reg. No. 34,929
Attorney of Record

408 884 1507
408 490 2853 FAX